VZCZCXRO3755
RR RUEHAT
DE RUEHAT #0083/01 3021646
ZNR UUUUU ZZH
R 291646Z OCT 09
FM AMCONSUL AMSTERDAM
TO RUEHC/SECSTATE WASHDC 1545
RUEHPNH/NVC PORTSMOUTH 0079
INFO RUEHAT/AMCONSUL AMSTERDAM 1579

UNCLAS SECTION 01 OF 04 AMSTERDAM 000083

SIPDIS

DEPT FOR CA/FPP
DHS FOR CIS/FDNS
DEPT PASS TO KCC WILLIAMSBURG KY
DEPT PASS TO EUR/EX

E.O. 12958: N/A
TAGS: KFRD CVIS CPAS CMGT ASEC NL
SUBJECT: FRAUD SUMMARY - NETHERLANDS

REF: (A) STATE 57623, (B) AMSTERDAM 46, (C) AMSTERDAM 74

¶1. Per the instructions in Ref A, Amsterdam submits the following post summary of fraud-related activity during the period from March 1, 2009 to August 31, 2009 updating Ref B.

Country Conditions

¶2. The Netherlands is a highly developed European nation. In 2008, The Economist Intelligence Unit ranked The Netherlands the fourth most democratic country in the world. The CIA World Factbook estimates that Dutch per capita income in 2008 was approximately $40,000, more than Canada, Japan, or France.

¶3. The Netherlands has a well-structured and easily accessible social welfare system and is well known for its generous asylum policy. According to the UNHCR, 9,298 new asylum applications were lodged from January to August 2009 in The Netherlands. Recent controversy in Dutch society over racial integration and Muslim extremism in The Netherlands has led the Government of the Netherlands (GONL) to take measures to stiffen requirements for refugees and asylum-seekers. Immigrants from non-Western countries now face stricter requirements and must demonstrate knowledge of Dutch society, language, and culture by successfully passing the Dutch Immigration and Citizenship Test.

¶4. The Netherlands is considered a low fraud country. Host government corruption is very low; The Netherlands ranks eighth, behind Iceland and ahead of Australia, on Transparency International's 2008 Global Corruption Perceptions Index. Most government documents contain high-tech security features and are easily verifiable.

NIV Fraud

¶5. During the reporting period Amsterdam adjudicated 11,366 NIV applications from citizens representing 135 countries. 7,275 of the applicants were Dutch travelers whose purpose of travel did not meet Visa Waiver Program (VWP) requirements or who were not entitled to avail themselves of the VWP.

¶6. Post encounters a small amount of fraudulent low-tech documents submitted in support of NIV applications; most are fabricated employment letters or letters of invitation. Other fraud committed by applicants is associated with attempts to hide prior refusals by applying with passports with different names and birth dates. Post's Fraud Prevention Manger (FPM) discovered through IDENT that a recent Nepalese B1/B2 applicant submitted his application under a different name and date of birth than the one he used during a prior refusal in Nepal. The

applicant explained that, after he was initially refused an F visa in 2002, a visa handler in Kathmandu urged him in March 2004 to procure a Nepalese passport with a false name and date of birth in order to increase his chances of being issued an H2B visa. Post is coordinating follow-up with Embassy Kathmandu.

¶7. Twenty-three cases were referred to the Fraud Prevention Unit (FPU) for investigation. Of these cases, only the Nepalese applicant mentioned above was confirmed as fraudulent.

IV Fraud

¶8. Post processed more than 220 IV applications during the reporting period, roughly half of which involving TCNs. It is often difficult to determine the authenticity of TCN supporting documents. Post occasionally identifies fraudulent documents in the IV workload. FPU routinely uses LexisNexis Accurint to verify information or to create a new line of questioning during an interview.

DV Fraud

¶9. Post issued 81 DV visas during the reporting period, including 28 to TCN applicants. Problems periodically encountered with non-Dutch DV applicants include difficulties in verifying educational qualifications and in obtaining police records. For example, despite several attempts, one Eritrean applicant waited more than 7 months for a police record from Kenya, where he had spent several years as a refugee. Post occasionally encounters applicants who swear to the accuracy of

information included in application forms they admit they did not complete or even read.

ACS and Passport Fraud

¶10. Post handled 2,268 passport applications, of which 272 were EPDPs issued at post, and processed 318 applications for additional visa pages. An average of 50-75 lost and stolen passports are returned to post each month from the local Dutch police and/or Dutch Immigration. Post issued 200 CRBAs during the reporting period.

¶11. Several cases of suspected passport fraud were referred to FPU for further investigation. In one case, post collaborated with DS to resolve a four decades-long investigation into an American citizen who stole the identity of a suicide victim in 1969 in order to fraudulently secure a United States passport. The subject is currently awaiting extradition to the United States.

¶12. An increasing number of American citizens have been victimized by Advance Fee (419) and other internet-related fraud scams originating in the Netherlands. Most of these scams have a link to Nigeria or Ghana.

Adoption Fraud

¶13. Post occasionally provides passport services for Dutch parents who are in the process of adopting American children and have temporary child custody while the adoption is finalized. Adoptions from the United States are never final until the parents have had at least three home visits by the relevant social services office in The Netherlands. The adopted child leaves the United States with a limited validity passport, normally issued for one year, which needs State Department approval for renewal. A full-validity passport is not issued

until the adoption is final, and adoptive parents need to present the final adoption decree and new birth certificate when applying. Because an original court order from the originating state government conferring custodial rights is required for Post to process such passport requests, the likelihood of fraud is limited.

Use of DNA Testing

¶14. Post did not request DNA testing during the reporting period.

Asylum and other DHS Benefits Fraud

¶15. Post processed six asylum/refugee (Visas 92/93) cases during the reporting period.

Alien Smuggling, Trafficking, Organized Crime, Terrorist Travel
---

¶16. The Netherlands is both a destination and transit point for alien smugglers, traffickers, and organized crime groups. Post has no evidence that any have targeted the Consulate General in an attempt to facilitate travel to or operations in the United States. Post works closely with onsite Customs and Border Protection staff and immigration and airport contacts to follow trends related to these issues and remain current on information pertinent to identifying such opportunities for misuse of visa and passport application processes. Please refer to the related fraud reporting section on CAWeb for Amsterdam's Schiphol Airport Fraudulent Travel Report.
http://intranet.ca.state.gov/fraud/14273.aspx ?gid=686.

DS Criminal Fraud Investigations

¶17. The Consular Section has an excellent working relationship

with the Regional Security Office at the Embassy in The Hague. Amsterdam has been identified as a post to receive an A/RSO-I position should funding become available. There were no investigations conducted during the reporting period.

Host Country Passport, Identity Documents, and Civil Registry
---

¶18. Dutch passports are burgundy red, with the Coat of Arms of the Kingdom of the Netherlands emblazoned on the front cover. The words "EUROPESE UNIE" (English: European Union) and "KONINKRIJK DER NEDERLANDEN" (English: Kingdom of the Netherlands) are inscribed above the Dutch national coat of arms and the word "PASPOORT" (English: passport). The Model 2006 biometric passport features the ICAO biometric passport symbol on the bottom-right of the cover.

¶19. Dutch passports comply with European Union (EU) and ICAO security standards. Each of the 34 pages of the Model 2006 biometric passports features a "Shadow" water-mark of the Dutch national coat of arms and conical laser image perforations. Security features on the synthetic, polycarbonate biographical data page include a Kinegram image that changes shape and color,

a laser engraved image perforation of the bearer's photo, and micro-printing above the machine readable zone repeating the text "Koninkrijk der Nederlanden." A contact-free chip containing the same data stored in the Machine Readable Zone adds an extra level of security.

¶20. In response to an EU agreement calling for additional biometric data to combat identity fraud and misuse, the Dutch Ministry of Foreign Affairs instituted a policy on September 21, 2009, that all Dutch passport and identity card applicants must provide four fingerprints, two of which are stored in a microchip in the documents. Dutch diplomatic and civil service passports have included fingerprint data since June 2009. GONL plans to store the fingerprint data in a centralized location accessible by Dutch law enforcement agencies are the focus of heated public debate. See Ref C for additional information.

¶21. The Netherlands has invested heavily in technology in its efforts to forestall and intercept fraudulent travel. The Dutch Expertise Center for Identity and Document Fraud (ECID) maintains a massive physical archive and digital database of fraudulent materials - including travel documents - confiscated by the Dutch government. The ECID operates the National Documentation System (NDS), formerly the Verification and Identity System (VIS), a national database of lost and stolen passports and drivers' licenses. Using fax, telephone and e-mail links to the ECID, authorized Dutch users can quickly check passport and drivers' licenses against the NDS system to weed out mala fide applicants. NDS users include police bureaus, immigration services, the national credit bureau, the post office and all Dutch banks. More than ten million documents from more than 62 countries are recorded in the database. NDS contains only document serial numbers and expiration dates. Names and personal information are not entered into the system.

¶22. The Dutch operate the NDS database on a fee-for-service basis. In 1999, the Dutch offered the Fraud Prevention Unit free access to NDS, but we were unable to accept for computer security reasons. Through our contacts, however, we are able to run queries on a case-by-case basis. Each month, Post's FPU forwards serial numbers and expiration dates of all lost and stolen U.S. passports replaced at post to the ECID for entry into NDS.

¶23. Since its addition to the Consular Consolidated Database (CCD) in January 2009, Post has regularly utilized the Edison Travel Document database, a software application created and managed by the Dutch government. Edison, which provides a centralized library of foreign travel document images and descriptions of their security features, has improved Post's ability to detect possible forged or altered travel documents and thus prevent illegitimate travel.

Cooperation with Host Government Authorities

¶24. Post enjoys a high level of cooperation with host government counterparts. Post's FPU regularly meets with the

Royal Dutch Border Police, known as the Koninklijke Marechaussee (KMAR), at Schiphol International Airport to gather information on fraudulent documents and travel trends. This exchange of information, while comprehensive, has been kept low-key and informal at KMAR's request. Please refer to the related fraud reporting section on CAWeb for Amsterdam's Schiphol Airport Fraudulent Travel Report.
http://intranet.ca.state.gov/fraud/14273.aspx ?gid=686.

¶25. The Dutch also informally exchange information on alien smuggling, trends in illegitimate travel, and document fraud at

monthly meetings of The Netherlands Immigration Liaison Team (NIL). The NIL is comprised of the Dutch immigration service (IND), KMAR, and Dutch National Police (KLPD) representatives, as well as United States, British, Canadian and German Immigration Liaison Officers.

Areas of Particular Concern

¶26. Schiphol International Airport is the fifth busiest airport in Europe behind London, Paris, Frankfurt, and Madrid, with over 47 million passengers in 2008. As a major transportation hub and transit center it is a source of a wide range of fraud issues and other criminal activities. Please refer to the related fraud reporting section on CAWeb for Amsterdam's Schiphol Airport Fraudulent Travel Report. http://intranet.ca.state.gov/fraud/14273.aspx ?gid=686.

Staffing and Training

¶27. Post has availed itself of several fraud-related training opportunities in the last six months. In September 2009, a CA/FPP representative visited Amsterdam to train staff on the new Fraud Reporting System. Shortly thereafter an LES from Stockholm, on a TDY assignment to Amsterdam's ACS section, volunteered additional training as Stockholm is a pilot site for the reporting system. Later that month, post's Visa Section Chief attended the CA/FPP-organized Iranian Fraud Conference.

¶28. Post's FSN Investigator (FSNI) received fraud prevention training at FSI in 2006 and continues to enhance her skills by attending training sessions conducted by the local police, immigration officials, and other diplomatic mission fraud experts. Post's efforts to prevent fraud are successful in large part due to the vigilance of Post's FSNI and her good rapport with Dutch interlocutors. Post is currently seeking to provide FSI fraud prevention training for a back-up FSNI.
RUTERBORIES